No Respect.
Chief Information Security Officers Misunderstood and Underappreciated by Their C-Level Peers

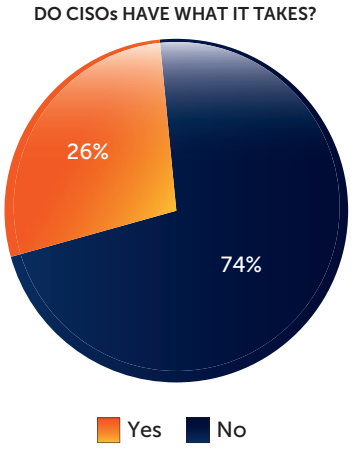
Summary

C-level executives regard the role of CISO primarily as a target for finger-pointing in the event of a data breach, and have little faith that individuals in the role could hold other leadership positions. Confusion about the role indicates that organizations must do a better job of understanding and elevating a position that is vital in the fight against cybercrime.

Despite their rising profile in recent years, Chief Information Security Officers (CISOs) still face a long climb in gaining the respect of many C-level executives. There is a prevailing notion that CISOs are primarily a scapegoat for security breaches, have not earned a seat at the senior leadership table and are unlikely to succeed in a leadership role outside of information security.

A ThreatTrack Security survey of 203 C-level executives at U.S.-based enterprises employing a CISO revealed that 44% of C-level executives believe CISOs "should be accountable for any organizational data breaches," but 54% believe CISOs should not be responsible for cybersecurity purchasing decisions. In other words, while CISOs deserve the blame for breaches in the minds of many executives, they should have limited say in acquiring the technology and resources to prevent them.

The perception of the CISO as scapegoat is especially prevalent among retail (65%) and healthcare (55%) companies – which are among the most common targets of cyber-attacks – as well as in the legal (67%) and professional services (52%) sectors. The sentiment in the retail sector may be explained, at least partly, by the aftermath of last year's Target data breach. More than half of all respondents (51%) – indicated they did not think it was "fair for Target to fire its CEO and CIO in the wake of the high-profile data breach."



Only 26% of C-level executives agree that CISOs should be part of an organization's senior leadership team.

Target divulged in December 2013 it had suffered a major security breach. The retailer originally reported the breach had compromised up to 40 million of its customers' credit and debit cards, but later adjusted the number to as many as 110 million. The company's CEO and CIO left the company shortly after the incident. It's instructive to note that Target did not have a CISO at the time of the incident; the company hired one in June 2014.

While enterprises are increasingly turning to CISOs to head their cybersecurity operations, about three quarters of respondents (74%) overwhelmingly said they do not believe that "CISOs deserve a seat at the table and should be part of an organization's leadership team." These findings reinforces the notion that CISOs are primarily viewed as convenient scapegoats in the event of a data breach,

and that their input – and by extension increasingly complex cybersecurity decisions – should not have a leading role in shaping corporate strategy.

No Respect

The ThreatTrack Security study uncovered clear signs that the role of the CISO has yet to achieve the level of respect and acceptance implied by the position's weighty responsibilities. After all, those responsibilities are directly linked to an organization's ability to prevent a security breach, which could bring substantial financial repercussions and even threaten a company's future.

The lack of confidence in the CISO appears related to a prevailing sense that individuals in that role are specialists with a narrow skillset. A clear majority of survey participants (61%) do not believe their CISO would succeed in a non-information security leadership position in their organizations. Asked whether "CISOs typically possess broad awareness of organizational objectives and business needs outside of information security," two-thirds (68%) did not agree.

61% *of executives do not believe their CISO would be successful in a leadership role outside of information security.*

Even within their area of expertise, CISOs have failed to win over all of their colleagues. Less than a third of respondents (27%) actually believe their CISO contributes greatly to improving day-to-day security, and 11% go so far as to affirm CISOs "provide limited value" in this regard.

However, 52% believe CISOs "provide valuable guidance to senior leadership related to cybersecurity." Nearly one-fifth of respondents (18%) view the role as primarily an advisor to the CIO on cybersecurity strategy. In that capacity, the CISO is allowed some influence on cybersecurity purchasing decisions, even though the prevailing attitude is they should not make those decisions themselves.

These findings seem to confirm there is confusion about the role of CISOs and the position's lack of clout: While CISOs have valuable insights, they are either failing to assert themselves or perhaps being ignored.

28% *of executives say a decision by their CISO has hurt their business' bottom line.*

At least some of that lack of confidence appears to be related to how a CISO's policies and initiatives impact the bottom line.

More than a quarter of respondents (28%) said their CISO has made cybersecurity decisions that have led to negative effects on the financial health of the organization, such as lost business, decreased productivity and impaired service levels. While these respondents comprise a minority, they still raise concerns: Are CISOs truly ineffective, or is the role so demanding that it becomes impossible to please all stakeholders? Do CISOs need to be more aware of how their actions impact the bottom line in order to gain more support in the executive leadership ranks?

HOW EXECUTIVES VIEW CISOs

CISOs should be responsible and accountable for all information security strategies and cybersecurity technology purchasing decisions.	46%
CISOs should be accountable for any organizational data breaches.	44%
CISOs are being hired to address critical gaps in organizations' information security capabilities.	31%
CISOs contribute greatly to improving day-to-day information security practices.	27%

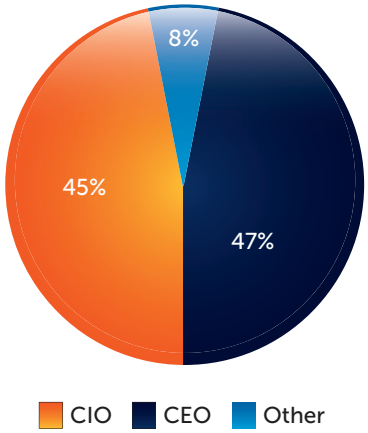
Opinions among executives are mixed on what a CISO's role in information security is and how effective they are.

Turf Battles

The ThreatTrack Security survey findings suggest a complicated relationship between CIOs and CISOs. A majority of CIOs (53%) agreed that CISOs should be responsible for all data breaches. In buying into the "CISO as scapegoat" characterization, these CIOs may have an ulterior motive: to protect their turf by deflecting blame for incidents to a lower-ranking position. In comparison, lower numbers of all other C-level executives responded in the affirmative to this particular question: 52% of CEOs, 35% of COOs and 43% of CFOs agreed CISOs deserve the blame for security incidents.

But while a majority of CIOs view CISOs as scapegoats, the same number of them (53%) said "CISOs should be responsible and accountable for all information security strategies and cybersecurity technology purchasing decisions." Perhaps giving CISOs purchasing responsibilities is another way for CIOs to put some distance between themselves and cybersecurity-related problems.

WHO DO CISOs REPORT TO?



Nearly half of CISOs still report to their organization's CIO, potentially limiting the effectiveness of these security leaders.

In contrast, 62% of CEOs, 42% of COOs and 41% of CFOs view cybersecurity purchasing decisions as part of the CISO's role. So even though CEOs will hold the CISO's feet to the fire in case of a breach, they seem to have more confidence in CISOs, which could make them better allies than CIOs.

Where CISOs sit within an organization chart may also play a role in shaping these opinions.

The study found that 47% of CISOs report to their CEO or president, while 45% report to the CIO, 4% to the Chief Compliance Officer, and less than 2% to the COO or CFO. Where CISOs report to the CEO or president, the corporate structure potentially lends itself to a turf battle between the CISO and CIO, which could help explain why more than half of CIOs buy into the scapegoat notion.

Average Grades

Asked to grade the overall performance of their CISOs, only 23% of participants gave their CISO an A for excellence. Almost three quarters of survey participants (72%) gave their CISO a grade of B or C in making their companies "more secure as it relates to stopping data breaches and combating sophisticated cyber threats." Only 5% of respondents gave them a D.

HOW DO YOU GRADE YOUR CISO?

A – Excellent	23%
B – Above Average	42%
C – Average	30%

CISOs receive passing marks, but opportunities remain for improvement as it relates to how executives view the job they are doing to secure organizations.

Once again, we see that CEOs have a more charitable attitude toward the CISO than the CIO, with 43% of CEOs giving their CISO an A, compared to just 22% of CIOs. CEOs, in fact, were the most generous on this question because outside their offices, A grades were mostly scarce.

Conclusion

CISOs carry the heavy burden of defending their organizations against unrelenting cyber threats; they unquestionably hold one of the toughest jobs in the corporate world. Speaking to the New York Times, one CISO compared the position to sheep waiting for the slaughter. As evidenced by ThreatTrack Security's survey findings, this characterization is entirely justifiable.

C-level executives, particularly CIOs, need to reconsider how they treat this relatively new position that didn't even exist a decade ago. The CISO is a highly-specialized role that few people have the knowhow and experience to undertake. As such, it should be elevated in the corporate structure to a level that corresponds to the post's weighty responsibilities. Treating CISOs as scapegoats is a self-defeating approach that may lead to complacency in addressing cybersecurity concerns.

Conversely, CISOs have a responsibility to prove themselves worthy of their seat at the leadership table. They must realize that as members of an enterprise's

senior leadership team, they have to demonstrate value beyond information security by aligning cybersecurity strategy with business goals – enabling the organization to succeed and reach its strategic objectives.

Study Methodology

The independent blind survey of 203 U.S.-based C-level executives – including CEOs, Presidents, CIOs, COOs, CFOs, General Counsels, Chief Legal Officers and Chief Compliance Officers in organizations that also employ either a CSO (Chief Security Officer) and/or CISO (Chief Information Security Officer) – was conducted by Opinion Matters on behalf of ThreatTrack Security between June and July of 2014.

About ThreatTrack Security Inc.

ThreatTrack Security specializes in helping organizations identify and stop Advanced Persistent Threats (APTs), targeted attacks and other sophisticated malware designed to evade the traditional cyber defenses deployed by enterprises and government agencies around the world. With more than 300 employees worldwide and backed by Insight Venture Partners and Bessemer Venture Partners, the company develops advanced cybersecurity solutions that **Expose**, **Analyze** and **Eliminate** the latest malicious threats, including its ThreatSecure advanced threat detection and remediation platform, ThreatAnalyzer malware behavioral analysis sandbox, ThreatIQ real-time threat intelligence service, and VIPRE business antivirus endpoint protection.

To learn more about ThreatTrack Security
call +1-855-885-5566 or visit www.ThreatTrackSecurity.com.

ThreatTrack SECURITY